Obserwuj nas na:

Nr 11/2020 (20)
Listopad 2020

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

MIASTO NIE MOŻE MIEĆ STAŁEGO DOSTĘPU DO BAZY DANYCH MPWIK

Obowiązujące przepisy prawa nie dają podstaw do tego, by organy podatkowe miały stały dostęp do danych o zużyciu wody przez wszystkich klientów firmy wodociągowej.

Przepisy ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach uprawniają jednostki samorządu terytorialnego do określenia metody ustalania opłaty za gospodarowanie odpadami komunalnymi. Jedna z nich może opierać się na wskaźniku ilości wody zużytej przez mieszkańców danej nieruchomości.

Plany weryfikacji deklaracji śmieciowych

Miasto, które zamierzało z niej skorzystać, planowało zwrócić się do działającego na jego terenie miejskiego przedsiębiorstwa wodociągów i kanalizacji (MPWiK) o możliwość stworzenia stałego dostępu do bazy danych zawierającej dane osobowe klientów oraz wskazujące na poziom zużytej w ich nieruchomościach wody. Chciało bowiem móc szybko weryfikować deklaracje składane przez mieszkańców miasta dla potrzeb określenia wysokości opłaty za gospodarowanie odpadami komunalnymi.

Rozważano, czy podstawą prawną dla takich działań nie mogłyby być przepisy ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa, umożliwiające organom administracji publicznej żądanie informacji o zużyciu wody w indywidualnych sprawach.

O wyjaśnienie, czy działanie takie byłoby zgodne z prawem, poproszono Prezesa UODO.

Do czego uprawniają przepisy podatkowe

Analizując sprawę, organ nadzorczy wziął pod uwagę m.in. przepisy ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, które zgodnie z art. 6q ustawy o utrzymaniu czystości i porządku w gminach, stosuje się w sprawach dotyczących opłat za gospodarowanie odpadami komunalnymi.

Wynika z nich, że uprawnienia organów podatkowych przysługują wójtowi, burmistrzowi lub prezydentowi miasta. Na ich podstawie (art. 82 § 1 ustawy – Ordynacja podatkowa) organ wykonawczy gminy może uzyskać od przedsiębiorstwa wodociągowo-kanalizacyjnego informacje o ilości wody zużytej przez mieszkańców. Osoby prawne, jednostki organizacyjne niemające osobowości prawnej oraz osoby fizyczne prowadzące działalność gospodarczą są bowiem obowiązane (zgodnie z art. 82 § 1 pkt 1 ustawy – Ordynacja podatkowa) do sporządzania i przekazywania informacji na pisemne żądanie organu podatkowego – o zdarzeniach wynikających ze stosunków cywilnoprawnych mogących mieć wpływ na powstanie obowiązku podatkowego lub wysokość zobowiązania podatkowego osób lub jednostek, z którymi zawarto umowę. Zgodnie zaś z art. 82 § 5 Ordynacji podatkowej, organ podatkowy określa zakres żądanych informacji oraz termin ich przekazania.

W swoich wyjaśnieniach Prezes UODO wskazał także na art. 82b § 1 Ordynacji podatkowej, który stanowi, iż organy administracji rządowej i samorządowej oraz państwowe i samorządowe jednostki organizacyjne są obowiązane współdziałać, nieodpłatnie udostępniać informacje w sprawach indywidualnych oraz udzielać pomocy organom podatkowym przy wykonywaniu zadań określonych w ustawie.

Istotne postanowienia RODO

Organ nadzorczy zwrócił uwagę, że w analizowanej sprawie istotne znaczenie ma nie tylko art. 6 ust. 1 lit. e RODO, stanowiący, że przetwarzanie jest zgodne z prawem wówczas, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, ale także motyw 31 RODO, który wskazuje, że organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe jednostki analityki

finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

Konkluzja

Biorąc pod uwagę powyższe regulacje, w opinii organu nadzorczego przekazanie całości informacji o zużyciu wody przez odbiorców innym organom niż prowadzące postępowania w sprawie egzekucji należności z tytułu nieuiszczonych opłat na podstawie wyżej wskazanych przepisów Ordynacji podatkowej byłoby nieuprawnione.

DO ORGANIZACJI PANELU OBYWATELSKIEGO NIE MOŻNA WYKORZYSTYWAĆ DANYCH Z REJESTRU WYBORCÓW

W opinii Prezesa UODO, gmina na potrzeby organizacji panelu obywatelskiego nie może wykorzystywać danych osobowych swoich mieszkańców, które są zawarte w rejestrze wyborców.

Panel obywatelski to nowa forma demokracji, która pozwala na podejmowanie decyzji na poziomie miasta, państwa, a także społeczności międzynarodowej. Rolą panelu obywatelskiego jest dogłębne przeanalizowanie danego tematu, omówienie różnych rozwiązań, wysłuchanie argumentów za i przeciw, a następnie podejmowanie świadomych i przemyślanych decyzji. Panele obywatelskie, w różnej formie, są organizowane na świecie od wielu lat.

Dla wiarygodności procesu kluczowe jest, aby panel był reprezentatywny pod względem demograficznym, a dobór osób wchodzących w jego skład odbył się w sposób rzetelny i transparentny. W tym celu przeprowadza się dwa losowania - w pierwszym losuje się osoby, które otrzymają zaproszenie do udziału w panelu. Jeżeli wylosowane w ten sposób osoby wyrażą zgodę na uczestnictwo, przeprowadza się kolejne losowanie, w którym typuje się ostateczny skład panelu. W pierwszym losowaniu musi zostać wylosowana taka grupa osób, która będzie odpowiadać strukturze demograficznej miasta w zakresie: płci, wieku i dzielnicy zamieszkania.

W Polsce dane dotyczące płci mieszkańców, wieku i dzielnicy, w której mieszkają, znajdują się w rejestrze wyborców. Stąd chętni, którzy zamierzają zorganizować panel obywatelski w jednym z miast w Polsce, zapytali Prezesa UODO, czy na potrzeby przeprowadzenia pierwszego losowania panelistów i panelistek można przetwarzać dane osobowe mieszkańców gminy organizującej panel obywatelski, które są zawarte w rejestrze wyborców.

W opinii Prezesa UODO, nie ma ku temu podstaw. Zgodnie bowiem z art. 18 § 4 ustawy z dnia 5 stycznia 2011 r. Kodeks wyborczy, rejestr wyborców służy do sporządzania spisów wyborców uprawnionych do udziału w wyborach, a także do sporządzania spisów osób uprawnionych do udziału w referendum. W myśl zaś art. 5 ust. 1 lit. b) RODO, dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (...). Wykorzystywanie rejestru na inne potrzeby niż przeprowadzenie wyborów naruszałoby zatem ową zasadę.

UDZIELANIE INFORMACJI PRZEZ OŚRODEK POMOCY SPOŁECZNEJ INNYM PODMIOTOM PUBLICZNYM

Podstawa prawna do przetwarzania, w tym udostępniania, danych osobowych przez podmioty publiczne powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami.

Podkreślić należy, że zgodnie z art. 100 ust. 1 ustawy z dnia 12 marca 2004 r. o pomocy społecznej, w postępowaniu w sprawie świadczeń z pomocy społecznej należy kierować się przede wszystkim dobrem osób korzystających z pomocy społecznej i ochroną ich dóbr osobistych. W szczególności nie należy podawać do wiadomości publicznej nazwisk osób korzystających z pomocy społecznej oraz rodzaju i zakresu przyznanego świadczenia. W ustępie 7 powołanego przepisu określono, że podmioty i osoby realizujące zadania w zakresie pomocy społecznej obowiązane są do zachowania w tajemnicy wszelkich informacji i danych, które uzyskały przy wykonywaniu tych zadań. Oznacza to, że dane osobowe przetwarzane przez ośrodki pomocy społecznej na gruncie ustawy o pomocy społecznej są chronione w sposób szczególny.

Zatem czy ośrodki pomocy społecznej mogą udzielać podmiotom publicznym, takim jak np. urząd gminy czy gminny ośrodek administracji szkół, które zwracają się do nich z wnioskami, informacji zawierających dane osobowe?

Tak, ale pod pewnymi warunkami. Przede wszystkim wskazać należy, że wszelkie działania podejmowane przez podmioty publiczne powinny mieć oparcie w obowiązujących przepisach prawa regulujących ich działalność. Wobec tego podstawa prawna do przetwarzania (w tym udostępniania) danych osobowych przez takie podmioty również powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami.

Właściwymi podstawami do przetwarzania (udostępniania) danych osobowych powinna być zatem przesłanka określona w art. 6 ust. 1 lit. c i e RODO w połączeniu z właściwymi przepisami szczególnymi określającymi zadania konkretnych organów i instytucji. Administrator powinien również ocenić, czy dane osobowe zawarte w informacjach, o które wnioskują podmioty publiczne, są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których mają być udostępnione. Nie wolno bowiem zapominać o konieczności realizacji zasady minimalizacji danych określonej w art. 5 ust. 1 lit. c RODO.

Oznacza to, że dane osobowe przetwarzane przez ośrodki pomocy społecznej na gruncie ustawy o pomocy społecznej są chronione w sposób szczególny.

Warto dodać, że rozpatrując wnioski o udostępnienie informacji zawierających dane osobowe administrator powinien współpracować ze swoim inspektorem ochrony. Jednym z jego zadań jest bowiem, w myśl art. 39 ust. 1 lit. a RODO, informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.

MIĘDZYNARODOWE

Rada Europy oceniła cyfrowe rozwiązania służące walce z COVID-19.

Raport „Rozwiązania cyfrowe w walce z COVID-19" opublikowany przez Radę Europy wskazuje szereg niedociągnięć w ochronie prywatności i danych osobowych w niektórych środkach prawnych i technicznych przyjętych przez rządy w celu zapobieżenia rozprzestrzenianiu się pandemii COVID-19 wśród 55 krajów Afryki, Ameryki Łacińskiej i Europy, które przystąpiły do Konwencji nr 108.

Raport zawiera analizę wpływu ram prawnych i polityk przyjętych przez rządy na prawa do prywatności i ochrony danych, a także dogłębną i techniczną analizę aplikacji do cyfrowego śledzenia kontaktów i narzędzia do monitorowania. Autorzy publikacji wezwali rządy do zapewnienia przejrzystości rozwiązań cyfrowych, aby zapewnić poszanowanie prawa do prywatności i ochrony danych. Pomimo licznych wezwań do koordynacji i interoperacyjności stosowanych rozwiązań cyfrowych w celu zapobieżenia rozprzestrzenianiu się pandemii COVID-19, kraje indywidualnie wdrażały rozbieżne systemy, ograniczając tym samym skuteczność podejmowanych działań.

Mając na celu ocenę zgodności przyjętych środków z konwencją o ochronie danych, sprawozdanie zawiera również zalecenia dotyczące sposobu zapewnienia skuteczności i odporności ram ochrony danych. W raporcie wskazano niedociągnięcia w zakresie przestrzegania zasad „Konwencji 108" w odniesieniu do takich kwestii, jak wymóg podstawy prawnej przyjętych środków, ich proporcjonalności oraz takich aspektów, jak uzasadnienie interesem publicznym i zgoda osoby, której dane dotyczą, do przetwarzania danych. Szczególnie trudnym aspektem jest ograniczenie celów przetwarzania danych. W raporcie wskazano również na zagrożenia dla ochrony danych związane z bezpieczeństwem, przechowywaniem i udostępnianiem danych.

Raport zawiera wyniki ankiety przeprowadzonej wśród państw-stron „Konwencji 108" w sprawie wykorzystania rozwiązań cyfrowych do kontroli rozprzestrzeniania się wirusa.

Analizując zgodność obecnie stosowanych przepisów z zasadą poszanowania prywatności, autorzy raportu zwrócili uwagę, że spośród 55 stron "Konwencji 108", 26 państw wybrało zdecentralizowane podejście do aplikacji śledzenia kontaktów, podczas gdy 14 wybrało podejście scentralizowane. Pięć krajów zdecydowało się w ogóle nie używać takich aplikacji. Spośród 47 respondentów biorących udział w badaniu ankietowym 36 korzysta z aplikacji do śledzenia kontaktów lub alertów zbliżeniowych (77%), 20 do autodiagnozy (43%), 11 do egzekwowania kwarantanny (23%), a 8 do mapowania wzorców podróży (17%). Tylko dwa kraje używały aplikacji do kontroli tłumu, a kolejne dwa do paszportów immunitetu.

Autorzy raportu z zadowoleniem przyjęli fakt, że 20 krajów biorących udział w badaniu opublikowało kody źródłowe aplikacji, co może przyczynić się do budowania zaufania użytkowników i zwiększenia skuteczności aplikacji.

Autorzy zalecają zaangażowanie społeczeństwa obywatelskiego i ogółu społeczeństwa w opracowywanie rozwiązań cyfrowych i środków przejrzystości, co może przyczynić się do wzrostu zaufania społeczeństwa do tych rozwiązań.

Komunikat prasowy: https://www.coe.int/en/web/portal/-/digital-solutions-to-fight-covid-19-shortcomings-protecting-privacy-and-personal-data

Link do raportu: https://rm.coe.int/report-dp--2020-en/16809fe49c

Hamburg: 35,3 mln euro dla Centrum Usługowego H&M

Hamburski organ ochrony danych nałożył administracyjną karę pieniężną w wysokości 35,3 mln euro za naruszenie ochrony danych osobowych w Centrum Usługowym H&M.

Sprawa dotyczy monitorowania kilkuset pracowników Centrum Usługowego H&M.

Firma zarejestrowana jest w Hamburgu i prowadzi centrum usługowe w Norymberdze. Co najmniej od 2014 roku spółka prowadziła szczegółową ewidencję informacji na temat niektórych pracowników pod kątem ich życia prywatnego. Notatki dotyczące pracowników były trwale przechowywane na dysku sieciowym. Po nieobecnościach pracowników wynikających z urlopów i zwolnień lekarskich, kierownicy zespołu nadzorującego przeprowadzali tzw. rozmowy powitalne z pracownikami (tzw. Welcome Back Talks). Po przeprowadzanych rozmowach w wielu przypadkach rejestrowano nie tylko informacje dotyczące konkretnych doświadczeń urlopowych pracowników, ale również objawów ich chorób i postawionych diagnoz.

Ponadto niektórzy przełożeni pozyskali szeroką wiedzę na temat życia prywatnego swoich pracowników podczas rozmów prywatnych i towarzyskich, od dość nieszkodliwych szczegółów, po kwestie rodzinne i przekonania religijne. Część tej wiedzy została utrwalona, zapisana w formie cyfrowej i częściowo udostępniona do odczytu dla 50 innych kierowników w firmie. Informacje te były czasami rejestrowane z dużą szczegółowością i przez dłuższy czas, dokumentując rozwój ewidencjonowanych zagadnień. Oprócz skrupulatnej oceny indywidualnej wydajności pracy, zebrane w ten sposób dane wykorzystano m.in. do uzyskania szczegółowego profilu pracowników w zakresie środków i decyzji podejmowanych w związku z ich zatrudnieniem. Połączenie zbierania szczegółowych informacji o ich życiu prywatnym i rejestrowania ich działań doprowadziło do szczególnie intensywnego naruszenia praw pracowników.

O zbieraniu danych przez spółkę dowiedziano się w październiku 2019 roku, gdy informacje te stały się dostępne w całej firmie na kilka godzin z powodu błędu w konfiguracji.

Hamburskiemu organowi ochrony danych przedstawiono kompleksową koncepcję wdrożenia ochrony danych w zakładzie w Norymberdze, od czasu stwierdzenia naruszenia. Jednocześnie kierownictwo firmy nie tylko wyraźnie przeprosiło pokrzywdzone osoby, ale również zastosowało się do sugestii, aby wypłacić pracownikom znaczne odszkodowania. Jest to bezprecedensowe przyznanie się do odpowiedzialności korporacyjnej po naruszeniu związanym z ochroną danych.

Źródło: https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en

Finlandia: kara za marketing bezpośredni bez uzyskania uprzedniej zgody

Rada ds. kar fińskiego organu ochrony danych nałożyła administracyjną karę pieniężną w wysokości 7 tys. euro na Acc Consulting Varsinais-Suomi (Independent Consulting Oy) za wysyłanie wiadomości marketingowych bez uprzedniej zgody odbiorców, jak również za zaniedbanie praw osób, których dane dotyczą.

W 2019 roku fiński organ ochrony danych otrzymał jedenaście skarg dotyczących marketingu bezpośredniego prowadzonego przez przedsiębiorstwo drogą elektroniczną oraz zaniedbania przez nie praw osób, których dane dotyczą.

We wniesionych skargach osoby, których dane dotyczą, zgłaszały, że otrzymywały od firmy wiadomości marketingowe, nie wyraziwszy na to zgody. Zgodnie z art. 200 fińskiego kodeksu społeczeństwa informacyjnego (917/2014) marketing bezpośredni może być skierowany wyłącznie do osób fizycznych, które wyraziły na to wcześniej zgodę.

Zgodnie z art. 4 ust. 11 RODO, zgoda musi być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli osoby, której dane dotyczą.

Niektóre z osób, których dane dotyczą, odpowiedziały na wiadomość marketingową wysłaną w formie wiadomości SMS zgodnie z żądaniem administratora danych w celu zaprzestania otrzymywania marketingu bezpośredniego. Pomimo wniesionego żądania do osób, których dane dotyczą, w dalszym ciągu kierowane były wiadomości marketingowe. W związku z tym administrator danych nie zapewnił możliwości realizacji prawa sprzeciwu osobom, których dane dotyczą, zgodnie z RODO. Administrator danych stwierdził, że numery telefonów osób, których dane dotyczą, były używane przez spółki, w której pracowały osoby, których dane dotyczą, oraz że spółki te należą do grupy klientów administratorów danych. Jednakże zdaniem organu ochrony danych, przed skierowaniem marketingu bezpośredniego, administrator danych powinien był oddzielnie określić pozycję danej osoby w korporacji, oceniając w szczególności, czy oferowane usługi były istotnie związane z obowiązkami danego pracownika. W związku z tym, marketingu bezpośredniego administratora skierowanego do osób fizycznych nie można uznać za przeznaczony dla korporacji, a administrator powinien był zwrócić się do osób, których dane dotyczą, o wyrażenie zgody na otrzymywanie informacji marketingowych.

Ponadto w niektórych skargach, osoby, których dane dotyczą, wskazywały na wnoszone żądania dotyczące realizacji ich praw zgodnie z RODO. Administrator nie odpowiedział na żądania osób zgodnie z terminami przewidzianymi w RODO - bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania - ani też nie zrealizował żadnego z nich. Fiński organ ochrony danych stwierdził, że w rezultacie administrator danych nie był w stanie udowodnić, że przetwarzał dane osobowe zgodnie z prawem.

Spółka nie odpowiadała na żądania dotyczące praw osób, których dane dotyczą, ani ich nie realizowała, a także nie była w stanie wykazać, że przetwarzała dane osobowe zgodnie z prawem.

Organ nadzorczy udzielił spółce upomnienia za zaniedbanie praw osób, których dane dotyczą, i niewdrożenie odpowiednich środków. Organ nakazał również spółce zmianę metod działania i wdrożenie środków umożliwiających wykonywanie praw osób, których dane dotyczą, zgodnie z wymogami RODO. Rada ds. kar fińskiego organu ochrony danych nałożyła, oprócz wymienionych środków naprawczych, karę pieniężną w wysokości 7 tys. euro. Rada ta uznała, że kara jest proporcjonalna i ma charakter odstraszający w odniesieniu do tego rodzaju naruszeń.

Decyzje fińskiego organu nadzorczego i Rady ds. kar nie są ostateczne, służy od nich odwołanie do sądu administracyjnego.

Źródło: https://edpb.europa.eu/news/national-news/2020/finnish-dpa-imposes-financial-sanction-company-due-carrying-out-electronic_pl

Norwegia: gmina ukarana za niewystarczające zabezpieczenie danych

Norweski organ ochrony danych wydał decyzje o nałożeniu administracyjnej kary na gminę Bergen w wysokości około 276 tys. euro. Dane osobowe wykorzystywane w systemie komunikacji między szkołą a domem nie były wystarczająco bezpieczne.

W październiku 2019 roku norweski organ nadzorczy został powiadomiony o naruszeniu ochrony danych osobowych przez gminę Bergen w związku z nowym narzędziem gminy do komunikacji między szkołą a domem o nazwie Vigilo. Zawiera ono moduł, w którym szkoła i rodzice mogą komunikować się za pośrednictwem portalu lub aplikacji. Gmina nie ustanowiła ani nie przekazała niezbędnych wytycznych w celu zabezpieczenia poufnych danych osobowych dzieci i rodziców, zanim narzędzie zostało użyte.

W decyzji nakładającej administracyjną karę pieniężną podkreślono, że gmina nie ustanowiła ani nie przekazała niezbędnych wytycznych dotyczących informacji o dzieciach, które mają wyraźny interes w przetwarzaniu informacji o nich z zachowaniem najwyższego stopnia poufności.

Dane osobowe, które powinny być poufne, zostały natomiast udostępnione osobom nieupoważnionym. W jednym przypadku lista kontaktów z informacją o „adresie poufnym" została przekazana rodzicom na poziomie klasy.

Komunikat prasowy:
- w języku angielskim: https://www.datatilsynet.no/en/news/2020/decision-to-fine-bergen-municipality/,

- w języku norweskim: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/endeleg-vedtak-om-gebyr-til-bergen-kommune/.

EDUKACJA

„Twoje Dane – Twoja Sprawa" pod tym hasłem od 11 lat UODO edukuje szkoły.

Działania edukacyjne i podnoszenie świadomości społecznej w zakresie ochrony prywatności obywateli są od lat, bardzo ważną częścią działalności organu ochrony danych osobowych. Obecnie unijne przepisy kładą ogromny nacisk na ochronę danych osobowych najmłodszych we wszystkich krajach UE. Wsparciem dla tego zadania jest z powodzeniem realizowany od 2009 roku ogólnopolski program edukacyjny UODO „Twoje dane – Twoja sprawa", którego XI edycja rozpoczęła się w październiku.

O kluczowych zasadach ochrony danych osobowych w placówkach edukacyjnych, a także o tym, jak realizowany jest program, przedstawiciele UODO rozmawiali ze szkolnymi koordynatorami programu podczas szkolenia online, które odbyło się 15–16 października 2020 r. Wzięło w nim udział ponad 200 osób.

Podczas wystąpień ekspertów UODO m.in. zostały omówione zagadnienia zgłaszane przez inspektorów ochrony danych z placówek oświatowych, odpowiedzi na bieżące pytania szkół, a także temat przygotowania odpowiednich procedur szkolnych w zakresie zgłaszania naruszeń. Natomiast liderzy programu, dzielili się swoim doświadczeniem, wiedzą i dobrymi praktykami w edukacji uczniów.

Popularyzacja wiedzy na temat skutecznej ochrony danych osobowych wśród uczniów i nauczycieli powinna być kluczowym elementem edukacji cyfrowej w szkołach. Wsparcie ekspertów – inspektorów ochrony danych w szkołach jest więc niezbędne w realizacji programu. Wielu inspektorów ochrony danych bierze udział w programie i dzieli się swoją wiedzą, doświadczeniem z nauczycielami oraz uczniami. Dzięki współpracy szkolnych koordynatorów programu z inspektorami ochrony danych w szkołach, organizowane są liczne spotkania z uczniami, a także powstają publikacje. Spotkania i szkolenia organizowane w szkołach stanowią ogromne wsparcie merytoryczne dla nauczycieli organizujących zajęcia z uczniami.

Więcej informacji o programie: www.uodo.gov.pl/tdts

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

Znajdująca się na naszej stronie internetowej zakładka „Inspektor Ochrony Danych" w sekcji „Zadania IOD" została wzbogacona o kolejne zagadnienia.

Wyjaśnienia dotyczą takich kwestii, jak:

Czy trzeba precyzyjnie określać okres przechowywania danych?
Czy trzeba dopełniać obowiązku informacyjnego wobec rodziny pracownika korzystającego z ZFŚS?
Jaki jest status projektanta w związku z wykonywaniem prac projektowych?
Czy z firmą szkoleniową trzeba zawrzeć umowę powierzenia?